BEST PRACTICES FOR BASIC CYBER SECURITY

Subject: Information Technology | **Current:** 2010 | **Grade:** 9-12 **Day:** 1 of 6

1 Purpose

To learn and understand the best practices for basic cyber security. These include best practices involving email, web surfing, and social networking.

2 Duration

Six hours. One hour each for the five topics listed in 9 B. below, and a sixth hour for closure and summary. Careers in Cyber security can be discussed in the sixth hour.

3 Additional Topics

Importance of cyber security for business, personal finance, and homeland security.

4 Objectives

Educate and prepare students in the safe, secure, and responsible use of computers and internet.

5 Standards Addressed

Demonstrate knowledge of security risks posed by the use of information technology and associated safeguards **IT.1.2.4**

Illustrate security risks and associated safeguards **IT.18.1.8**

Indiana Department of Education. (n.d.). Indiana Standards and Resources: Business, Marketing & Information Technology. Retrieved from http://dc.doe.in.gov/Standards/AcademicStandards/StandardSearch.aspx

6 Vocabulary

Cyber Security, malware, spyware and adware, viruses and worms, authentication, spam, spoofing

7 Materials

JMU Cyber Guide (http://www.jmu.edu/iiia/cybercitz/) and web sites (see Additional Resources). This file is attached.

8 Additional Resources

Websites: http://www.jmu.edu/iiia/cybercitz/ , www.staysafeonline.org

9 Procedures & Methods

Lecture, Discussion and hands-on review of websites.

A. Introduction

The teacher gives an overview of cyber security and its importance to our personal and financial information and how it relates to security of our private and governmental.

B. Development

The following six areas should be covered in six lessons, one in each:

1. Introduction and General Safety Tips:

- Cover the material in pages 2-3 of the JMU Cyber Guide.
- Involve students in a discussion where students relate their experiences and knowledge about general safety tips.

2. Digital Communications Safety:

- Cover pages 4-7 of the JMU Cyber Guide.
- Make an assignment to have students write a one-page description of their experiences about digital communications safety.

3. Social Networking

- Cover pages 8-9 of the JMU Cyber Guide.
- Have students discuss their experiences with social networks and what they like and do not like about those.

4. Emerging Technology

- Cover pages 10-11 of the JMU Cyber Guide.
- Discuss chat abbreviations and let student come up with some new ones.

5. Surfing the Web

- Cover pages 11-12 of the JMU Cyber Guide.
- Ask students to describe their web surfing experiences.

6. Review of the topics covered above. If time remains, topics from pages 14-20 of the JMU Cyber Guide may be covered.

C. Practice

The instructor works with the students as a team to study and discuss the JMU Cyber Guide.

D. Independent Practice

Each student selects a cyber security web site. This could be one of the sites mentioned in this lesson. The student then prepares a report discussing five facts about cyber security found from the resource.

E. Accommodations (Defferentiated Instruction)

For students who have difficulty with comprehension issues, a graphic organizer such as a Venn diagram or a compare/contrast chart may be used Students who have visual, mobile or hearing impairments may need adaptive computer software to assist with using the computer and accessing the websites for information. Students who need extra scaffolding may need a graphic organizer to use in understanding the information and to provide a more concrete way to complete the Practice portion of the lesson. High ability/gifted students may want to go further in depth in any of the topics.

F. Checking for Understanding

The students list 3-5 best practices in each area of cyber security covered in the lesson, and describe the advantages of following those best practices.

G. Closure

Almost all careers and jobs that involve the use of computers and applications such as office productivity software, email, and use of internet browsers require knowledge of best practices in cyber security. In particular best practices in software security are required knowledge for careers involving software and hardware management. These careers incluwde software engineers, computer engineers, web developers, system administrators, programmers, and software testers.

For more details, students should visit the following websites:

http://www.edu.com/articles/careers-in-cyber-security/

http://www.dhs.gov/xabout/careers/gc_1240512546017.shtm

10 Evaluation

1. The teacher assigns each student to select ten concepts from those covered in Lessons 1-6 and write a report that contains a one paragraph description of each concept.

2. The student writes a one page description of careers in cyber security based on the information from the web site http://www.dhs.gov/xabout/careers/gc_1240512546017.shtm or another website the student discovers on her/his own.

11 Teacher Reflection

To be completed by the teacher after completing the lesson.

12 Section Title

- JMU Cyber Guide (http://www.jmu.edu/iiia/cybercitz/) and web sites
- http://www.jmu.edu/iiia/cybercitz/
- www.staysafeonline.org
- http://www.edu.com/articles/careers-in-cyber-security/
- http://www.dhs.gov/xabout/careers/gc_1240512546017.shtm